In re: Application of	Victor Gorelik
Application No.	10/725,116
Filed	12-02-2003
Title	TWISTED SIGNATURE
Examiner	LOUIE, OSCAR A
Art Unit	2109

Appeal Brief

Table of Contents

(i) Real party in interest.

The real party in interest is inventor Victor Gorelik.

(ii) Related appeals and interferences.

None.

(iii) Status of Claims.

Claims 1-5 are rejected under 35 U.S.C. 102(b) as being anticipated by Buffam (US-6185316-B1).

(iv) Status of Amendments.

No amendment filed subsequent to the final rejection.

(v) Summary of claimed subject matter.

Not included: the appellant is not represented by a registered practitioner.

(vi) Grounds of rejection to be reviewed on appeal.

Not included: the appellant is not represented by a registered practitioner.

(vii) Argument.

Rejection under 35 U.S.C. 102(b) over U.S. Patent No. US-6185316-B1.

Claims 1 to 4.

The ground for rejection is improper because Buffam's invention and my application have absolutely different goals and use different ways of achieving these goals.

The goal of Buffam's invention is security of the server. Buffam uses biometric data and a special method of encoding to improve this security to the highest possible level.

The goal of my application is privacy of the user in the case if security of the server is broken, which is beyond Buffam's consideration.

In Buffam's method the claimant receives access to the server only if he/she provides correct (real) biometric data and correct plain text (password known to the user only). So, if the system lets the attacker in, he/she knows that submitted/generated biometric data is real, and the attacker can use this data for purposes other then access to this particular server.

In my method the claimant receives access to the server if he/she submits a shuffled array of real biometric data. The sequence of values in this shuffled array is defined by the user during the enrollment phase. This shuffled array, not the real one is the proxy of the user. So, if the system lets the attacker in, he/she knows only that he/she has submitted the correctly shuffled array of biometric data, not the real biometric data. Attacker can try to determine the original sequence of values in real biometric data array by using the method of trial and error. However, the number of possible pairs "trial original sequence – trial permutation" producing the same sequence (which was defined during enrollment and opens access to the server) may be very big, and the attacker does not have a way to find out which of these pairs contains the original sequence of values and which does not.

The fact that there are many additional solutions giving access to the server does not mean that it is easy to find even one of them. However, it means that if such a solution is found, it probably does not reveal the real biometric, and there is no way to figure out which solution reveals the real biometric and which does not.

To summarize: the method of trial and error can restore real biometric data in Buffam's invention, because there is only one input which opens access to the server, however, this method is useless in my application, because there are too many inputs, which open access to the server.

This is the main difference between Buffam's encoding and my shuffling in this context.

Let us consider the following simplified example.

The real biometric data of the user is the set of three points e.g. (10, 11), (22, 23), (34, 35), which can be treated as two arrays: the first for x-coordinates – 10, 22, 34, and the second for y-coordinates – 11, 23, 35.

According to Claim 1 of my application the user shuffles these 2 arrays. Let us suppose, to shuffle the first array (10, 22, 34) the user applies permutation 2, 3, 1 and receives array (22, 34, 10); to shuffle the second array (11, 23, 35) the user applies permutation 3, 1, 2 and receives array (35, 11, 23). As a result, the user has three new points: (22, 35), (34, 11), (10, 23) instead of the real ones: (10, 11), (22, 23), (34, 35).

According to Buffam's invention two new false points, e.g. (46, 47) and (58, 59), are added to the set, so there are 5 points now: (10, 11), (22, 23), (34, 35), (46, 47), (58, 59).

Claim 2 of my application states that the new sequence is calculated at the client based on information known to the user only. For this simplified example it means that both permutations – 2, 3, 1 and 3, 1, 2 – are not calculated or stored anywhere – they are determined at the client on the basis of the value of the twister known only to the user.

In Buffam's invention 2 false points are calculated on the basis of the 3 real ("true") points at this step.

According to Clam 3 of my application the arrays of biometric data may be multiplied by the sequences of numbers known at the client only, which in case of multiplying sequence e.g. {3, 10, 2, 7, 1,-1} and twisted points (22, 35), (34, 11), (10, 23) produces points (66, 350), (68, 77), (10, -23). These three new points are the proxy of the user. They are submitted and saved at server during enrolling phase.

In Buffam's invention plain text known to the user only (e.g. "Sesame, open up!") along with 2 false points (46, 47), (58, 59) are used as input for encoding. The output is a cipher text. This cipher text along with 5 points (3 true and 2 false): (10, 11), (22, 23), (34, 35), (46, 47), (58, 59) are saved at the server during the enrollment phase.

Claim 4 of my application describes the process of verification. This process does not include decoding. Biometric data is twisted at the client and only this twisted data is submitted to the server. Information which was used to twist the data (two permutations and sequence of multipliers) is not submitted to the server. Verification is being done by comparison of twisted data submitted by the claimant against the data stored on server. If the claimant submits exact the same twisted data: (66, 350), (68, 77), (10, -23), he is the right person and access to the account is granted. Because of the non-deterministic nature of biometric sampling, calculation of correlation coefficient may be used instead of direct comparison.

In Buffam's method claimant submits real biometric points plus plain text. These points are compared with 5 points stored at the server. Coinciding points are removed; the remaining points plus submitted plain text are used to produce the cipher text. In case if the claimant is the right person, she/he submits true points (10, 11), (22, 23), (34, 35) that will be removed from the union of five points (10, 11), (22, 23), (34, 35), (46, 47), (58, 59) stored on server. Two remaining points (46, 47), (58, 59) and the plain text are used to produce the cipher text. Because the claimant is the right person, this cipher text will coincide with the cipher text stored on server. So, access to account will be granted.

One purpose of this simplified comparison is illustration of the fact that every one of my 4 claims is different from Buffam's invention:

- claim 1 describes the shuffling of coordinates of true points instead of creating additional false points,
- claim 2 states that this shuffling is done on the basis of information known only to the user instead of calculation of new false points;
- claim 3 is additional multiplication of the coordinates instead of producing encoding key from the false points and plain text;
- claim 4 is a comparison of submitted twisted data against twisted data stored on the server instead of calculating the cipher text on the basis of submitted real biometric data and plain text.

The second purpose of this comparison is even more important for my arguments. It is the proof (as follows below) that real biometric data can be restored using the data stored on the server in case of Buffam's method and cannot be restored in case of my method.

Indeed, if the attacker generates some wrong biometric data points e.g. (1, 1), (2, 2), (3, 3) or some wrong plain text e g. "Let me in, please", the Buffam's procedure will reject the claim. However, if the attacker generates correct data points (10, 11), (22, 23), (34, 35) and correct plain text "Sesame, open up!" (randomly or using new mathematical methods – it does not matter how), the Buffam's procedure will remove these 3 points from the 5 points stored on the server, and use two remaining points and plain text to produce the cipher text, coinciding with the cipher text stored on the server. So, access to the account will be granted, and – which is the main point of my argument – the real biometric information: (10, 11), (22, 23), (34, 35) will be revealed.

In case of my method the attacker also can randomly generate correct array of biometric data: (10, 11), (22, 23), (34, 35), correct permutations: 2, 3, 1 and 3, 1, 2, and correct multiplying sequence: {3, 10, 2, 7, 1,-1), opening access to the server. However, the attacker would not know that he/she has generated real array of biometric data. There are always other combinations ("additional solutions"), which will open access to the server as well. To make reasoning easier let us assume that there is no additional multiplication, or, the same, that all multipliers are equal to 1: {1, 1, 1, 1, 1, 1}, not {3, 10, 2, 7, 1,-1). In this case there are 36 (36=3!*3!) different solutions:

(10, 11), (22, 23), (34, 35), with permutations 2, 3, 1 and 3, 1, 2;

(22, 11), (10, 23), (34, 35), with permutations 1, 3, 2 and 3, 1, 2;

(34, 11), (10, 23), (22, 35), with permutations 3, 1, 2 and 3, 1, 2;

and so on, opening access to the server. Each of these solutions produces twisted sequences (22, 35), (34, 11), (10, 23) saved on server. Only the first of these 36 solutions has the real biometric data (10, 11), (22, 23), (34, 35).

In case of using additional multipliers (as proposed in claim 3) the number of possible solutions increases in great degree.

The fact that there are many additional solutions giving access to the server does not mean that it is easy to find even one of them. However, it means that if such a solution is found, it probably does not reveal the real biometric, and there is no way to figure out which solution reveals the real biometric and which does not.

So, the main difference between Buffam's and my methods in real-world operations is that in Buffam's method the real biometric data is collected at client and submitted to the server; in my method twisted biometric data is collected at client and submitted to the server.

As a result of this difference, if Buffam's method is used, it is possible to restore real biometric data if security of the server is broken; if my method is used, it is impossible.

Rejection under 35 U.S.C. 102(b) over U.S. Patent No. US-6185316-B1.

Claims 5.

Additional note of the Examiner to this claim is that the only "means" of "means-plus-function' language are computer program modules, so 35 U.S.C. 112 6th paragraph has not been invoked.

In my understanding claim 5 describes means for implementing methods of claims 1-4. Example of means different than computer program module is given in the very end of the Detailed Description of the Invention: "For example, teller machines may store twisted fingerprints of the customer, generated based on the real fingerprints and secret code known to the customer only."

If the Examiner or a member of the Board could advise better wording for claim 5, I would gratefully accept it.

(viii) Claims appendix.

What I claim as my invention is:

Claim 1. A method for securely submitting biometric data from a client to a server comprising the steps of:

performing sampling of a real biometric characteristic at the client; and

shuffling arrays of real biometric characteristics in the sequence known at client only to thereby generate twisted biometric data; and

submitting the twisted biometric data from the client to the server.

Claim 2 A method according to claim 1 wherein the shuffling sequence is calculated at client on the basis of the value of a secret object created at the client and known to client only.

Claim 3. A method according to claim 2 combined with the step of multiplying the arrays of biometric characteristics by the sequences of numbers fixed for each type of array and known at the client only.

Claim 4. A method according to claim 3 wherein the step of submitting of twisted biometric data is followed by the step of comparing this data against the samples of twisted biometric data saved at the server previously, in such a way, that the result of the verification and/or identification depends neither on the specific sequence in which biometric arrays were shuffled on the client, nor on the specific sequence of numbers used on the client to change the values of the arrays.

Claim 5. A system for secure use of biometric data comprising: the means for performing twisted sampling by changing the sequence of terms in biometric array and submitting data to the server, said system programmed for performing verification and/or identification of the client.

(ix) Evidence appendix.

None.

(x) Related proceedings appendix.

None.

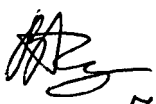
(xi) Conclusion.

In his response to my amendment Examiner states:

- "Applicant's argument regarding Claim 1 is non-persuasive since the shuffling of sequence **is equivalent** to hushing, encrypting, encoding, etc."
- "Arguments regarding Claim 2 are non-persuasive since the combining of hashed false image points and true image points would succeed by means of a **similar** procedure as "shuffling" of a sequence of values in a biometric array."
- "In regards to the applicant's argument to Claim 3, the two procedures as disclosed by Buffam and the applicant are **equivalent**."
- "The applicant's arguments in regard to Claim 4 are non-persuasive because in the context of Buffam decoding is **equivalent** to a comparison of two twisted signatures."
- "In regard to Claim 5, the invention as disclosed by Buffam is **equivalent** to the applicant's invention."

The Examiner conducted the above comparison of two methods from the point of view of security of the server. However, the main goal of my method is ensuring the privacy of the user if security of the server is already broken. My method guarantees that in this case there is no way to restore real biometric data of the user. In case of Buffam's method the real biometric data can be restored by the attacker and can be used for purposes other then access to this particular server.

In this brief I am not making new arguments. I am repeating my argument I have never received a response to: my method and Buffam invention are **not equivalent or similar** from the point of view of the user's privacy. As I explained in the amendment, "the privacy of the user is assured in greater degree in my method. I believe this difference presents patentable novelty which the claims present in view of the references cited (Buffam, US-6185316-B1) and the rejection made ("anticipation")."

Inventor  V.Gorelik.

7/9/2007